COALITION WARRIOR INTEROPERABILITY DEMONSTRATION 2011

TRIAL 2.32 – MANAGING MILITARY CIVILIAN MESSAGING (M2CM)

Summary Report

August 2011

Compiled and Edited by

Edgewood Chemical Biological Center
NBC Battlefield Management Branch

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 AUG 2011	**Final**	**01 Jun 2011 - 30 Aug 2011**

4. TITLE AND SUBTITLE
Wide Area Recovery and Resiliency Program (WARRP) CWID 2011 Trial 2.32 - Managing Military and Civilian Messaging Summary Report

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ginley, William

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Edgewood Chemical Biological Center NBC Battlefield Management Branch Aberdeen, MD 21001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Lori Miller Department of Homeland Security Science and Technology Directorate Washington, DC 20538

10. SPONSOR/MONITOR'S ACRONYM(S)
DHS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
6.4.0

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
Coalition Warrior Interoperability Demonstration (CWID) is a Chairman of the Joint Chiefs of Staff-directed annual event that engages cutting-edge information technology, focusing on operational shortfalls identified by combatant commanders and government agencies. Technologies are approved for participation because they address a new information sharing capability or potentially improve an existing capability. The demonstrations, which take place in various locations worldwide, focus on technology discovery, risk reduction, and coalition interoperability. CWID 2011 Trial 2.32 supported CWID Objective 2 to enhance the whole of Government integration and interoperability in order to improve cyber operation and support sustainable secure mission partner collaboration. Trial 2.32 dealt with Managing Military Civilian Messaging (M2CM). M2CM is a system of systems approach to address the need for rapid information sharing between military and civilian emergency management communities. M2CM employs a mix of program of record, commercial and Science and Technology (S&T) applications/tools to provide end-to-end communications.

15. SUBJECT TERMS
WARRP, Military Communications, Civilian Communications, Managing Military Civilian Messaging, M2CM, CWID

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**38**	

EXECUTIVE SUMMARY

The Edgewood Chemical Biological Center (ECBC) NBC Battlefield Management Branch (NBC BMB) and their partners demonstrated Military-Civilian information sharing during the Coalition Warrior Interoperability Demonstration (CWID) 2011. Trial 2.32 – Managing Military Civilian Messaging (M2CM) is a system of systems approach to address the need for rapid information sharing between military and civilian emergency management communities. NBC BMB partnered with multiple organizations both Military and Civilian to integrate a representative group of Military and Civilian Incident Management tools that could be used to demonstrate representative message exchange between the Military and Civilian communities. The Department of Homeland Security's Science and Technology Office (DHS S&T) sponsored trial teamed the NBC BMB with the Joint Program Manager for Information System (JPMIS), PM Guardian, Monmouth University Rapid Response Institute (RRI), Space and Naval Warfare Systems Command (SPAWAR), Federal Emergency Management Agency (FEMA) Integrated Public Alerting and Warning System (IPAWS), Buffalo Computer Graphics, Indiana University of PA, Opti-Metrics, Compass, and PM Installation Protection Program.

Trial 2.32 - M2CM employed a mix of program of record, commercial, and Science and Technology (S&T) applications/tools to provide end-to-end communications. Military First Responders on scene and Military Stabilization Forces (NG, Army Reserve) operating an Incident Command Post (ICP) were able to generate and share Allied Data Publication No. 3 (ADatP-3) messages with a Military Emergency Operations Center (EOC) running JPM Guardian's Decision Support Services (DSS) 5.0 and Command and Control Personal Computer (C2PC) with Joint Warning and Reporting Network (JWARN). The ADatP-3 military messages were translated into Common Alert Protocol (CAP) using the Remote Message Center (RMC) Translation Tool. The messages were then shared with the Civilian EOC via the Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN). The representative civilian incident management tool, Disaster LAN, was used to issue alerts via CAP messages to Military and Civilian Emergency Operation Centers (EOC). The RMC was used to translate the CAP messages received from the Civilian EOC and pass the resultant ADatP3 messages within military channels. Emergency Data Exchange Language (EDXL) Resource Messages (EDXL-RM) were also generated and shared using the RMC. Trial 2.32 - MC2M addressed the information sharing beginning at the sensor in the field up to the Emergency Operations Center. Wireless networks, nuclear, biological, chemical and first responder sensors, and common military and civilian planning tools were used to generate and share information. This allowed the team to play an all hazards response using messaging that is germane to either the civilian or military communities.

The successful nine day CWID demonstration was the result of eight months of planning, coordination, integration and testing. The planning and coordination included the participation in three CWID planning conferences, development of detailed mission scenario event lists (MSELs), and training of role players. A training team traveled to the Delaware Army National Guard (DEARNG) facility in Smyrna, DE to provided training prior to CWID execution. The primary integration effort was enabling RMC, Disaster LAN, and ICBRNE to share messages via IPAWS OPEN. In preparation for CWID, the Trial 2.32 – M2CM technologies were set up at ECBC to provide a test bed for the integration, MSEL development, and training material development. During CWID execution Trial 2.32 – M2CM was represented at multiple sites (Herndon, San Diego, Hanscom, and NORTHCOM) with the main location being the DHS Battle Lab in Herndon, VA.

During the nine days of scenario play, Trial 2.32 – M2CM was successful in meeting the primary objective to demonstrate the exchange of information across a combination of existing military, civilian, and emerging S&T Tools. Role players from the National Guard were trained on the various technologies (i.e., JWARN, JPM Guardian's Decision Support Service 5.0, Disaster LAN, JWARN, Remote Message Center, etc…) and successfully generated, sent, and received CAP, EDXL-RM, and ADatP-3 messages using the Civilian and Military tools.

Table of Contents

1.0 Introduction

The Edgewood Chemical Biological Center (ECBC) NBC Battlefield Management Branch (NBC BMB) and their partners demonstrated Military-Civilian information sharing during the Coalition Warrior Interoperability Demonstration (CWID) 2011. Trial 2.32 – Managing Military Civilian Messaging (M2CM) is a system of systems approach to address the need for rapid information sharing between military and civilian emergency management communities. NBC BMB partnered with multiple organizations both Military and Civilian to integrate a representative group of Military and Civilian Incident Management tools that could be use used to demonstrate representative message exchange between the Military and Civilian communities. The Department of Homeland Security's Science and Technology Office (DHS S&T) sponsored trial teamed the NBC BMB with the Joint Program Manager for Information System (JPMIS), PM Guardian, Monmouth University Rapid Response Institute (RRI), Space and Naval Warfare Systems Command (SPAWAR), Federal Emergency Management Agency (FEMA) Integrated Public Alerting and Warning System (IPAWS), Buffalo Computer Graphics, Indiana University of PA, Opti-Metrics, Compass, and PM Installation Protection Program.

The successful nine day CWID demonstration was the result of eight months of planning, coordination, integration and testing. The planning and coordination included the participation in three CWID planning conferences, development of detailed mission scenario event lists (MSELs), and training of role players. A training team traveled to the Delaware Army National Guard (DEARNG) facility in Smyrna, DE and provided training prior to CWID execution. The primary integration effort was enabling the Remote Message Center (RMC), Disaster LAN, and Integrated Chemical, Biological, Radiological, Nuclear and Explosive (ICBRNE) Program to share messages via IPAWS Open Platform for Emergency Networks (OPEN). In preparation for CWID, the Trial 2.32 – M2CM technologies were set up at ECBC to provide a test bed for the integration, MSEL development, and training material development. During CWID execution Trial 2.32 – M2CM was represented at multiple sites (Herndon, San Diego, Hanscom, and NORTHCOM) with the main location being the DHS Battle Lab in Herndon, VA.

The following pages will provide an overview of the CWID demonstration, a description of Trial 2.32 – MC2M, a brief description of the technologies employed in Trial 2.32, and a summary of the efforts associated with planning and execution of CWID Trial 2.32. Lessons learned associated with each technology used during CWID will be discussed as well as lessons learned associated with the integrated process.

2.0 Coalition Warrior Interoperability Demonstration Overview

CWID is a Chairman of the Joint Chiefs of Staffs-directed annual event that engages cutting-edge information technology, focusing on operational shortfalls identified by combatant commanders and government agencies. Technologies are approved for participation because they address new information sharing capability gaps or improve an existing capability. The demonstrations, which take place in various locations worldwide, focus on technology discovery, risk reduction, and coalition interoperability. CWID 2011 consisted of five U.S. locations and more than 20 coalition partners worldwide. The CWID Enterprise consists of multiple venues hosted by the United States, Canada, and the North Atlantic Treaty Organization (NATO), designed to improve and enhance Command, Control, Computers, Communications systems, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities. U.S. Government, Department of Defense, first response agencies and multinational counterparts all sponsored technologies, called Interoperability Trials (IT), into CWID consistent with the Warfighter defined objectives. Technologies are assessed using operationally inspired Warfighter, Homeland Security/Homeland Defense and emergency responder scenarios. During demonstrations, technologies may receive three types of assessments which include User Utility, Interoperability and Information Assurance. Assessment results are captured in CWID's annual assessment report which informs the defense, federal and state acquisition communities with decision-quality data. The final report is published annually each November. The annual demonstration

evaluates technologies and their capabilities for exchanging information among coalition partners, military services, government agencies, first responders and U.S. combatant commanders. Information sharing technologies influence decision-making and operational flexibility on the battlefield, and during crisis response on the home front. While the focus of CWID is new and emerging commercial technologies, CWID is also a venue for government information technology development or validation of fielded or near-fielded commercial, DoD and partner systems.

3.0 Trial 2.32 – Managing Military Civilian Messaging Objectives

Trial goals and objectives were identified early and presented during the CWID Initial Planning Conference in November 2011. The CWID 2011 Goals and Interoperability Objective for Trial 2.32 - M2CM are:

- CWID 2011 Goals
    - To demonstrate a seamless exchange of messages between civilian and military responders
    - To successfully demonstrate S&T message exchange concepts in a realistic scenario based environment
- Interoperability Objective
    - To demonstrate the exchange of information across a combination of existing military, civilian, and emerging S&T Tools (i.e., JWARN, JPM Guardian's Decision Support Service 5.0, Disaster LAN, Remote Message Center, etc…)

4.0 Trial 2.32 Description

Trial 2.32 - M2CM employed a mix of programs of record, commercial, and S&T applications/tools to provide end-to-end communications. DEARNG and NJ National Guard playing the role of Military First Responders on scene and Military Stabilization Forces (NG, Army Reserve) operating an Incident Command Center (IOC) were able to generate and share Allied Data Publication No. 3 (ADatP-3) messages with a Military Emergency Operations Center (EOC) running JPM Guardian's Decision Support Services (DSS) 5.0 and Command and Control Personal Computer (C2PC) with Joint Warning and Reporting Network (JWARN). The ADatP-3 military messages were translated into Common Alert Protocol (CAP) using the RMC Translation Tool. The messages were then shared with the Civilian EOC via the Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN). The representative civilian incident management tool, Disaster LAN, was used to issue alerts via CAP messages to Military and Civilian Emergency Operation Centers (EOC). The RMC was used to translate the CAP received from the Civilian EOC and pass the resultant ADatP3 messages within military channels. Emergency Data Exchange Language - Resource Messages (EDXL-RM) were also generated and shared using the Remote Message Center (RMC). Trial 2.32 - MC2M addressed the information sharing beginning at the sensor in the field up to the Emergency Operations Center. Wireless networks, nuclear, biological, chemical and first responder sensors, and common military and civilian planning tools were used to generate and share information. This allowed the team to play an all hazards response using messaging that is germane to either the civilian or military communities. Figure 1 depicts the System View 1 (SV-1) for Trial 2.32.

Trial 2.32 – M2CM participated at four of the CWID sites; DHS Battle Lab, NORTHCOM, SPAWAR, and Hanscom AFB. The DHS Battle Lab in Herndon was the primary site and all of the M2CM technologies were represented. A limited support presence was at SPAWAR with JWARN, ICBRNE, and RMC being demonstrated. Hanscom and NORTHCOM were virtual sites where only RMC was being exercised and support was provided remotely.

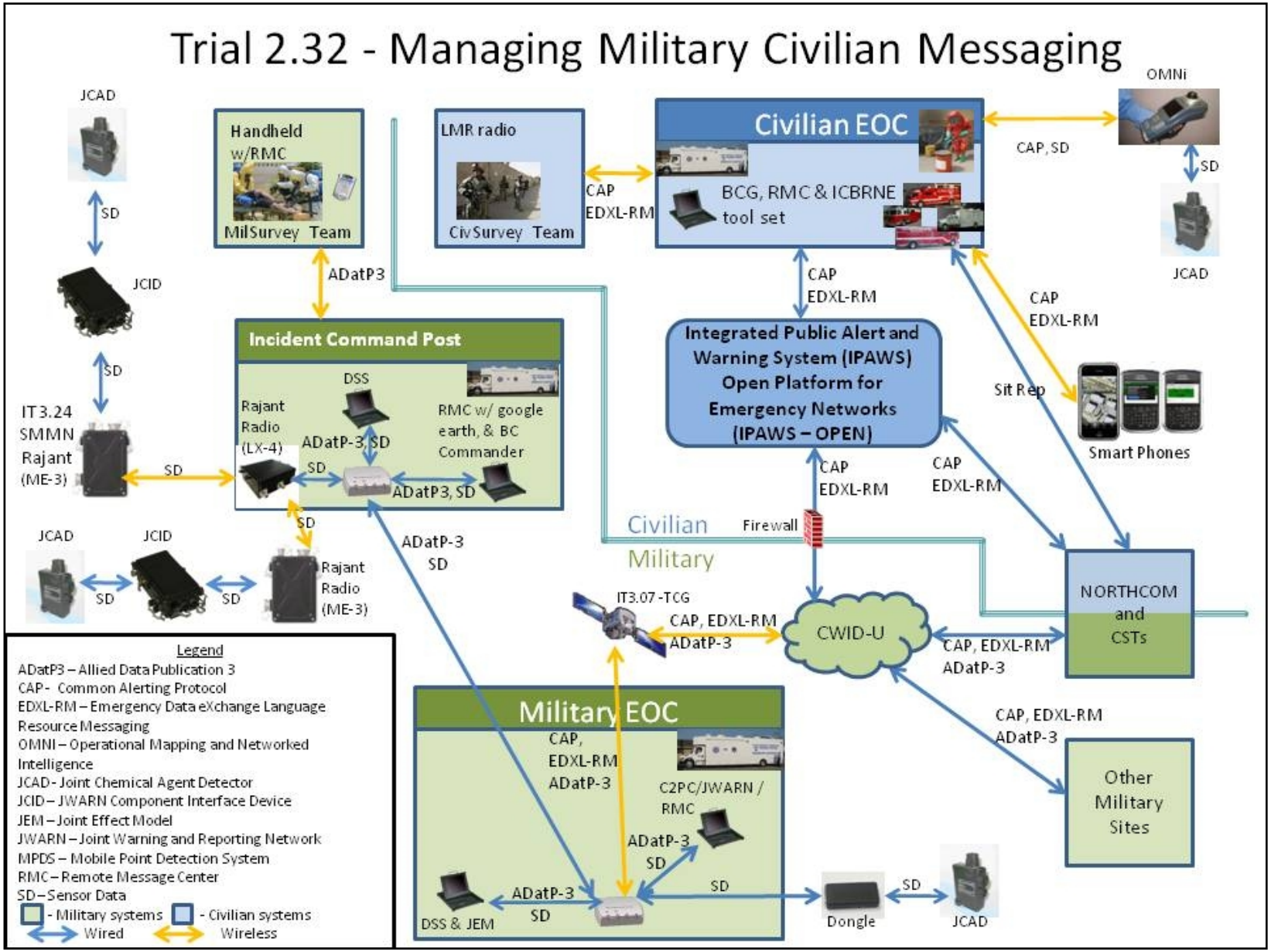

Figure 1- Trial 2.32 System View

Trial 2.32 – M2CM was setup in two locations at the DHS Battle Lab. Inside the facility RMC was loaded on the DHS provided workstations to support the various National Guard Bureau roles. The Joint Mobile Command and Training Center (JMCTC) truck was located in the DHS Battle Lab parking lot and served as the Incident Command Post (ICP)/ Emergency Operation Center (EOC). All the software and hardware tools associated with Trial 2.32 were available and used in the JMCTC truck. A Rajant radios was also co-located at trail 3.07's van for connection to their system.

5.0 Software Components

The focus for selecting software tools for CWID 2011 was to identify representative civilian and military incident/emergency management systems. The software systems selected were a combination of emerging S&T Tools, beta versions of enhanced fielded software, and program of record developmental software.

5.1 Civilian Systems

Two civilian systems were a critical part of the CWID event, IPAWS OPEN and Disaster LAN. IPAWS OPEN provided the pathway to exchange CAP and EDXL-RM messages and Disaster LAN served as the representative Civilian Emergency Management system.

5.1.1 Integrated Public Alert and Warning System Open Platform for Emergency Networks

Description: Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN) is a non-proprietary operational interoperability backbone that acts as a "level playing field" to allow disparate third-party applications, systems, networks and devices to share information in non-proprietary, open standards based format. As Federal infrastructure, IPAWS-OPEN is designed to support the delivery of real-time public alerts, emergency data, and situational awareness data to the public and to emergency responders in the field, at operation centers, and across all levels of response management. The IPAWS-OPEN test environment serves as test bed to facilitate the development of open non- proprietary standards to support interoperable information sharing for the emergency responder community. The IPAWS-OPEN production environment provides the operational capability to share standards based messaging in CAP and EDXL formats.

System Performance: The IPAWS-OPEN supported the operation successfully throughout the entire nine day exercise. There was not a point in time where the services provided by IPAWS-OPEN 2.0 failed. There were delays that typically incurred in processing of network data causing severe latency. This obstructed the ability to successfully share information. The long delays were causing IPAWS-OPEN 2.0 to time out resulting in unsuccessful transmissions. Upon discovering network latency it was decided to move the network over to the Monmouth University command vehicle's satellite receiver and messages began moving effectively.

Monmouth University's Android application was not handling COGs effectively. The programmer's (doctoral students) were on constant standby throughout the operation to remedy any situation. In one evening they rewrote a segment of the application in order to successfully transport CAP and EDXL-RM messages.

The decision was made by the IPAWS Program Office just prior to CWID to move the M2CM from the IPAWS OPEN development environment to the production environment. In the long run this was a benefit since we were operating in a more stable environment, but there was a loss with respect to test time for dry runs of the MSELs.

The MSELs timing was not well planned and could have been improved if additional time was available for dry runs.

Lessons Learned:

- Maintain closer coordination with the IPAWS Program Office to ensure we are aware of potential programmatic requirements that may impact testing.
- Provide more time to train role players.
- Provide more role players to run the systems.
- Try to recruit at least two additional vendor applications that support IPAWS-OPEN 2.0 to be used for civilian support.

5.1.2 Disaster LAN™

Description: Disaster LAN™ is a state-of-the-art web-based crisis information management system designed for use in emergency operations centers. Designed by emergency managers, for emergency managers, Disaster LAN™ provides an easy-to-use interface based upon the workflow requirements of the emergency management community. Disaster LAN™ is fully NIMS compliant and highly secure. It is used by agencies at state, county, and local levels, as well as by private corporations.

Disaster LAN™ can be deployed at a fixed facility, as a mobile solution, or as a virtual solution in the Buffalo Computer Graphics data center. Because of Disaster LAN's™ web-based architecture, anyone with a functioning Internet connection and proper security privileges can immediately participate in incident management via the world-wide-web. This means that members of the emergency management team can participate in crisis management activities from locations outside the physical EOC. It also means that as the incident grows in size; additional personnel can be brought into the "virtual EOC" with a few clicks of the mouse button. Disaster LAN™ can share critical information between a local EOC and state or federal partners instantly and securely.

In order to accommodate the diverse needs of the emergency management community, Disaster LAN™ has been developed in a modular configurable fashion. This allows each Disaster LAN™ installation to be custom tailored to the specific needs of the customer. Some of the features/modules available in Disaster LAN™ are: Call Center; Call Center Management; Report Generator; 24/7 Event Monitoring Center; Incident Coordinators; User Lists; Internal Messaging; Interoperable Messaging; Message Broadcasting; etc… In support of the CWID event, Buffalo Computer Graphics integrated with IPAWS OPEN and implement the CAP 1.2 standard.

Disaster LAN's™ was accessed from the JMCTC truck during CWID execution using the truck satellite to connect to the Internet and also via a wireless air card. The primary capability demonstrated was the ability to send and receive CAP and EDXL-RM messages via IPAWS OPEN and email.

System Performance: The messaging portion of Disaster LAN™ is a straight forward application that is easy to learn and easy to use. Being a web-based system, Disaster LAN™ is highly dependent on the stability and speed of the network. The original plan was to access the CWID network via Trial 3.07 or through a wireless access point on the DHS Battle Lab building. Both approaches were not functional during the CWID event, and the JMCTC truck satellite was the available internet access point. The satellite bandwidth was limited and there was suspected hardware issues with the laptop causing Disaster LAN™ to virtually come to a stop. The decision was made to run from a standalone laptop using a Verizon Wireless Air Card and performance was greatly improved.

The implementation of the IPAWS OPEN interface and the email exchange of CAP and EDXL-RM messages was a work in progress during the CWID planning and execution. The Buffalo Computer Graphics developer provided

rapid response to the issues that were identified during CWID. The issues that were identified were typical for a development environment such as formatting incompatibility between RMC and Disaster LAN's™. For example, minor modifications were required on both RMC and Disaster LAN™ to provide two way email exchange of messages.

Only selected fields in the resource message were implemented in Disaster LAN™ and the fields selected did not provide sufficient information to support any action by an incident manager. These fields can be tailored by a system administrator, but there was not enough time to fully evaluate and determine the appropriate fields to display.

The MSEL play called for the entry of GPS coordinates to map out polygons such as staging areas, road blocks, etc… Disaster LAN™ initially only allow placement of a shape using placement by locating a position on the map with cursor and adding a radius for a circle or dragging and clicking to add additional points for a polygon. Buffalo Computer Graphics modified the interface to allow placement by adding a GPS coordinate and radius.

Lessons Learned: The lessons learned related to Disaster LAN™ are primarily related to refining the GUI for the CAP and Resource Messages.

Need to review the Resource Message Standard and identify the critical fields required for a useful message. This goes along with the comment associated with the Remote Message Center that a thorough review of the standard is needed to remove redundant fields to simplify data entry.

5.1.3 Integrated Chemical, Biological, Radiological, Nuclear and Explosive Program

Description: The Integrated Chemical, Biological, Radiological, Nuclear and Explosive Program (ICBRNE) allows civilian and military emergency operation centers to share messages with each other and send messages to other agencies. During the CWID Demonstration ICBRNE sent CAP messages to the Civilian EOCs via the Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN). The messages were then forwarded via IPAWS OPEN to RMC where they were translated and distributed within military channels.

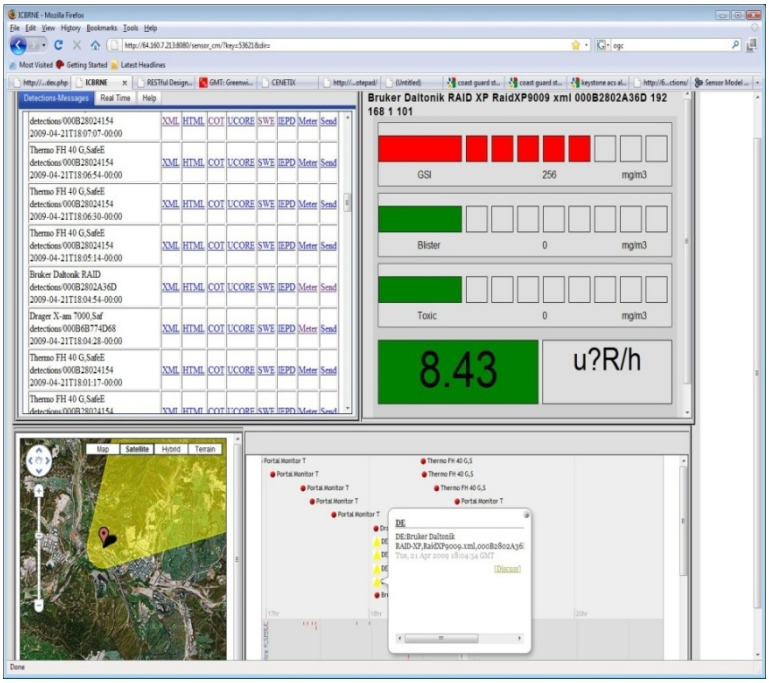

Figure 2 - ICBRNE

The M2CM trial involved similar hardware and software setups at both the Herndon and San Diego sites. The hardware included first responder sensors, Wi-Fi dongles for the sensors, a sensor laptop, a laptop to post messages to OPEN, mobile tablets, and a mobile Wi-Fi hotspot. The software included sensor monitoring software, software to poll the ICBRNE web server, and ICBRNE apps for the mobile tablets.

Setup issues: At times, the sensor software would show a working connection to the sensors but the sensor readings would no longer refresh. These were fixed by restarting the sensor laptop. There were issues with the iPad and the Wi-Fi hotspot overheating, but this was due to Herndon weather. This was fixed by bringing the devices inside the truck and restarting them. GPS on our sensors was not always fully functional. This was fixed by virtualizing coordinates into the sensor software XML, which was required for MSEL play anyway as some alerts had to originate from other locations in the country. Sometimes sensors would clearly alarm but would require significant time above alarm thresholds before alerts would show up on the server. The tablet screens had poor visibility in sunlight. The Wi-Fi hotspot speed would sometimes feel slow. This was fixed by closing background tabs in the laptop browser windows and by closing background apps on the tablets.

System performance: The ICBRNE system was functional. Alerts were sent to the ICBRNE server and subsequently posted to OPEN during MSEL exercises as expected. A lot of this can be credited to the system being independent of the other networks, because we were running our devices on a Wi-Fi hotspot. Sometimes the sensors would have to be triggered above the alarm threshold for up to a minute instead of a few seconds to trigger alerts because of the refresh rate of the polling software. Early in MSEL play, it was sometimes difficult to distinguish which messages were for MSEL play and which were the result of demos or testing. This was fixed by editing the CAP messages to display exercise numbers in addresses and headlines so that the exercise messages could be quickly spotted in the other system software.

Lessons learned: It was good to have an independent network to run our system on, but obviously this is not possible for every system. When network issues were at their worst, communication between groups was key, but it was especially important to have good communication with sites on opposite ends of the country. The ICBRNE teams in Herndon and San Diego could have a better system to communicate. IM was good when both parties were on, but there was not a clear indication of whether a person was really at the computer or not so it could take several minutes for responses to questions.

Recommendations: It would be good if there could be a system showing what MSEL exercise number each player was currently working on. This was not a big issue since we were only sending outgoing messages and we were not affected by incoming messages from other systems, but it would be good to receive confirmation that our outgoing messages were actually received.

5.2 Military Software

Six military software tools were identified and used during CWID 2011; the Remote Message Center, JWARN, C2PC, Joint Effects Model (JEM), Decision Support System, and CIMS.

5.2.1 Remote Message Center

Description: The Nuclear, Biological, Chemical Remote Message Center provides Allied Technical Publication (ATP-45 (C)) functionality. ATP-45 defines two warning and reporting roles: the source (ATP-45 Section 1, Paragraph 0107) and the collection center (ATP-45 Section 1, Paragraph 0108). RMC provides the functionality necessary for survey and reconnaissance teams to fulfill the objectives of the source role. It allows the user to create attack reports (NBC1), create detection reports (NBC4), and receive hazard reports (NBC3 and NBC5). The tool

also includes import, export, and email features for communication with command and control systems used by chemical officers at the collection center. When an appropriate NBC report is received, RMC can process the report and export the geo-referenced hazard area on a digital map. The RMC program supports visualization of hazard overlays via the Keyhole Markup Language (KML). Google Earth was used as an example of an application that can read the KML overlays generated by the program. Figure 3 shows the RMC basic interface.

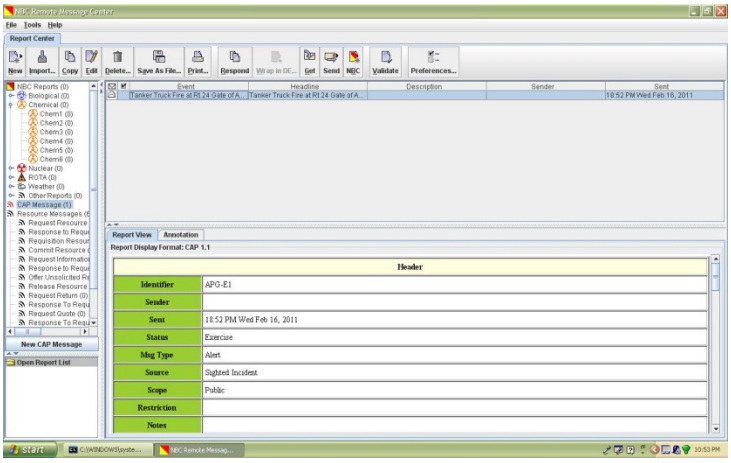

Figure 3 – RMC Interface

The Remote Message Center was upgraded to include the CAP (Figure 4) and EDXL-RM messaging capability and was integrated with IPAWS OPEN. The transition capability that was added to the Remote Message Center enabled CAP messages to be transitioned to ADatP-3 or USMTF formatted messages, specifically NBC SitReps. NBC messages can be transitioned to CAP messages. NBC-3 messages which include hazard predictions can be transitioned to CAP messages that include the hazard prediction as a polygon. The EDXL-RM messages can be transitioned to a NBC SitRep, but there is no transition from a NBC SitRep to a resource message. During CWID, the core capabilities provided by RMC enabled the exchange between the Civilian and Military. RMC was deployed and successfully demonstrated at four CWID sites: DHS Battle Lab, San Diego, Hanscom, and NORTHCOM.

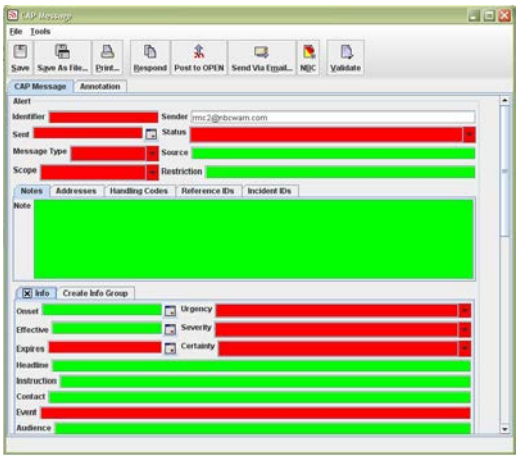

Figure 4 – RMC CAP Template

CWID 2011 provided a venue to introduce and test the RMC with National Guard operators in support of the transition to the Wide Area Recovery and Resiliency Program (WARRP), and JPM IS. In coordination with WARRP, and agreement with JPM IS, an appropriate transition exercise or demonstration will be selected to provide a venue for completion of the transition. JPM IS will issue an acceptance memorandum upon successful completion of the event.

System Performance: The Remote Message Center performed consistently throughout the CWID demonstration. Two methods of sharing messages were used with the Remote Message Center. CAP and EDXL-RM messages were shared as an embedded message in an email or via an IPAWS OPEN posting. NBC messages were shared with JWARN as an embedded email.

There were a few issues related to set-up experienced at each CWID site. Specifically, establishing email addresses for each of the instances of the Remote Message Center created some operational confusion. The connection to the CWID Network couldn't be established from the JMCTC truck so the decision was made to establish Gmail accounts for the various duty stations in the truck and in the DHS Battle Lab. Over the course of the initial days at CWID, there were numerous instances of email addresses being mistyped or duty positions being assigned two email addresses and the wrong address was used to send a message.

The most critical issue that was identified was timing. Each instance of the Remote Message Center polls IPAWS OPEN for new CAP and EDXL-RM messages. Any messages that have an earlier date stamp than the last message received will be ignored. The Remote Message Center adjusts to Zulu time so the time zones are accounted for, but if the sending and receiving machine times are out of sync messages can be lost. This is particularly a concern when short auto-polling intervals are set or when rapidly manual polling.

There was a minor issue related to the format of the COG addressing that caused messages not to be delivered when multiple COGs were address.

Lessons Learned: There were several lessons learned associated with the Remote Message Center.

Timing – A method to account for out of sync system times needs to developed. One approach would be to poll OPEN for message older then the last pole. The Remote Message Center already compares messages so any duplicates would be ignored, but if a message was deleted prior to the second polling the unwanted message will be posted to the Remote Message Center.

Resource Message Standard – The RM standard is large with duplicate fields that enable the user to enter information in a multiple of locations based on preference. The standard needs to be thoroughly reviewed and compared to the Remote Message Center GUI to streamline the GUI and make the interface easier to use.

5.2.2 Joint Warning and Reporting Network

Description: The Joint Warning and Reporting Network (JWARN) is the Program of Record for standardized nuclear, biological and chemical (NBC) warning and reporting that will provide Joint Forces with a comprehensive analysis and response capability to minimize the effects of NBC attacks or accidents/incidents. JWARN uses NBC warning technology to collect, analyze, identify, locate, report and disseminate NBC threat information. Compatible and integrated with Joint Service C4ISR systems, JWARN will be located in Command and Control Centers at the appropriate level and will be employed by NBC defense specialists and other designated personnel. JWARN transfers data automatically to and from the actual detector/sensor and provides commanders with analyzed data for disseminating warnings to the battlefield level. JWARN provides data processing, plans and reports as well as access to specific NBC information to improve the efficiency of limited NBC personnel assets.

JWARN provides the capability to report CBRN and Toxic Industrial Materials (TIMs) hazard detection by collecting, generating, editing, and disseminating NBC plots and reports on Command and Control (C2) platforms to provide a Common Operational Picture (COP) for the Warfighter. JWARN also provides the Joint Force Commander with the capability to analyze detections to enable identification of the hazard and plot affected locations. Inherent in JWARN is the capability to auto-generate ATP-45 hazard Warning Areas and through JWARN's connection to JEM generate more detailed hazard area plots. JWARN disseminates warning and de-warning information to affected units, provides archiving event data for later evaluation, and controls/configures the local sensor networks.

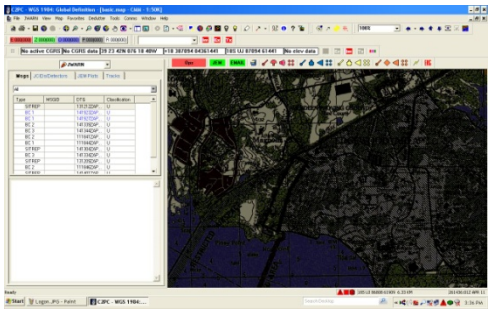

Figure 5 – C2PC/JWARN Interface

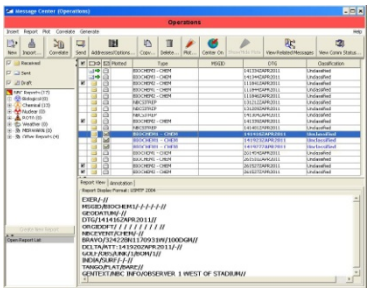

Figure 6 – Message Center

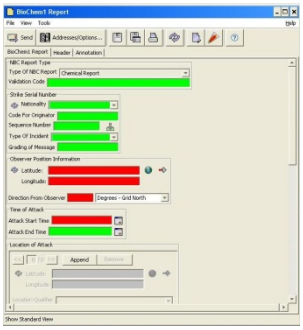

Figure 7 – NBC Message Template

System Performance: During CWID execution, C2PC was the C2 platform used with JWARN and JWARN was deployed at the DHS Battle Lab in the JMCTC truck and in San Diego at the SPAWAR CWID site. In general there were no critical issues with JWARN during the demonstration. Operators were able to create NBC-1 messages correlate to a NBC-2, plot the NBC-2, generate and save the NBC-3, and then send the NBC-3 to another instance of JWARN or the Remote Message Center.

Two issues were experienced during the demonstration. The email set-up issue where multiple accounts were assigned and the wrong one used to send messages caused some missed messages early in the demonstration. There was an issue related to the anti-virus and network lockdowns that caused an interruption in the receipt of messages. The Norton anti-virus was turned off and messages were being received.

Lessons Learned: The NBCBMB has a great deal of experience working with JWARN and there were no major issues experienced during the CWID event.

5.2.3 Joint Effects Model

Description: The purpose of the Joint Effects Model (JEM) is to provide Department of Defense (DOD) agencies with a single accredited modeling and simulation program that can provide hazard areas and effects results for Chemical, Biological, Radiological, and Nuclear (CBRN) weapons and incident effects from Toxic Industrial Chemicals / Toxic Industrial Materials (TICs/TIMs) that can be displayed directly on existing and future Command, Control, Communications, Computers, and Intelligence Surveillance, and Reconnaissance (C4ISR) systems.

JEM combines the best components from existing CBRN Science and Technology (S&T) models (such as HPAC, VLSTRACK, and D2PUFF) and integrates selected current capabilities of them into a common operating architecture, interoperable system, and user interface. The software system elements of JEM are the shared infrastructure and the user interfaces such as the interoperability with the JWARN and common C4ISR systems, Common Operating Environment (COE) systems, and Common Operational Picture (COP) systems.

JEM is designed to predict and track CBRN and TIC/TIM releases to:

1. Support operational decisions and risk assessments for the Passive Defense, Force Protection, Consequence Management, and Homeland Security mission areas.

2. Support the intelligence preparation of the battlespace and the development of operational options, including conventional attack and special operations planning and interoperating with C4I systems to facilitate information sharing.

3. Support planning to mitigate the effects of WMD.

4. Assist DoD components, as well as allied or coalition forces, by providing CBRN and TIC/TIM hazard predictions and effects to the Warfighters during and after an incident.

5. Assist DoD components, as well as allied or coalition forces, to train jointly; develop doctrine and tactics; and assess warfighting, technology, materiel development proposals, and force structure.

System Performance: During CWID execution, JWARN was deployed at the DHS Battle Lab in the JMCTC truck and in San Diego at the SPAWAR CWID site. There were no issues with JEM during the demonstration. Operators were able to generate and display hazard predictions as scripted. Figure 8 illustrates a JEM Hazard prediction displayed in C2PC/JWARN.

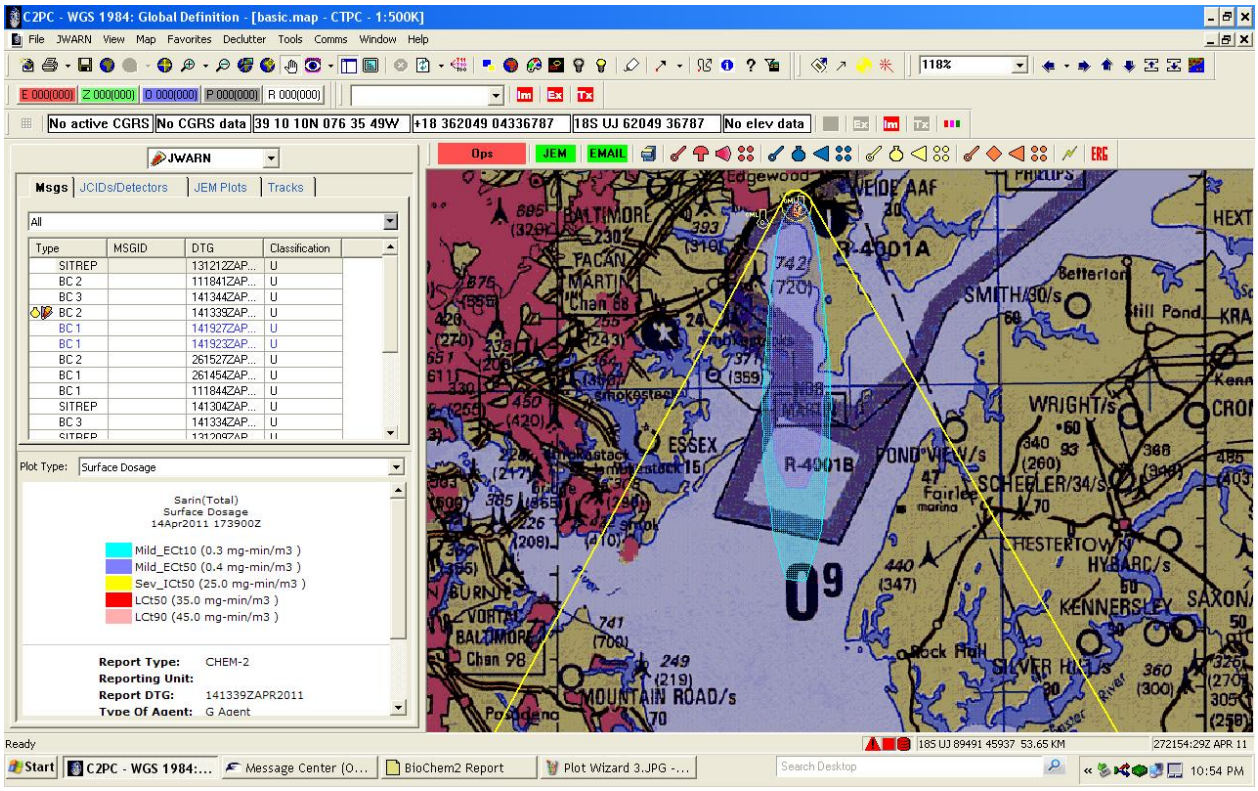

Figure 8 – JEM plot

Lessons Learned: The NBCBMB has a great deal of experience working with JEM and there were no issues experienced during the CWID event.

5.2.4 Decision Support System (DSS)

Description: Decision Support System was designed for DoD installations (Guardian Program) as a Web-enabled system based on the National Incident Management System (NIMS) guidance. DSS is an integrated system that provides a fully functioning Chemical, Biological, Radiological, and Nuclear (CBRN) focused, all hazards capable, incident management capability allowing Emergency Operations Center personnel and incident first responders to share near real-time information with each other and with installation decision-makers. DSS consists of two main components, one for the EOC and one for the ICP. The EOC component provides the installation with situational awareness display for the command group and the tools needed to handle emergencies to warn/protect personnel and property while still continuing the installation's mission and return it back to normal operations quickly. The ICP component is basically Cobra software modified to communicate with the EOC piece. ICP is used by the first responders to help coordinate the incident response and provide the necessary tools, databases, checklists and forms to help get the incident under control. The concept of implementation is that an ICP component is stood up for each incident across the installation and the EOC maintains overall installation situation awareness and coordinates with each ICP.

The Trial 2.32 implementation of DSS consisted of four laptops. The computer resources available required the backbone of the system to be placed on two laptops (usually done on one computer) that contained the Domain Controller, Open Street Map Server and the Web & Database Server. The other two laptops were used to run the EOC and ICP pieces which communicate internally with each other. The four laptop configuration is a non-standard deployment of DSS that was implemented because ECBC did not have laptops of sufficient capability to support the standard configuration.

DSS was only deployed at the DHS Battle Lab and was housed in the JMCTC truck. For demonstration purposes, both the ICP and EOC components were located inside the JMCTC.

System performance: The DSS system performance can be broken into Startup, DSS internal information exchange, and external information exchange.

Startup – Operating out of the JMCTC required the team to shutdown the equipment each night during CWID and restart DSS each morning. At startup the ICP and EOC had difficulty synchronizing and the system appeared to be running slow. A set of troubleshooting procedures were followed each day that enabled the EOC and ICP to synchronize. Once the EOC and ICP synchronized, this issue would not appear again. The DSS program office provided on site technical support on several occasions and with their help the hardware was determined to be at the low end of the acceptable performance range for running DSS. The apparent cause for the issue is that DSS was not fully up and running when we tried to synchronize between the ICP and EOC. Given the low end hardware and that there was not a clear indication that DSS was fully loaded, we were not waiting a sufficient amount of time before trying to synchronize. Once DSS synced up, this issue would not appear again. To improve the performance of the laptop, several services that were not being used during the exercise were turned off, and log files were removed to free up some hard disk space.

DSS Internal Information Exchange - DSS functioned as advertised with respect to exchange of information between the EOC and ICP components. The DSS toolset is design to support incident management exchange of information between the ICP and EOC, and provide base situational awareness. DSS fulfilled those functions without any issues.

External Information Exchange – DSS is setup to export and import files, but the capability is limited. In general information from external sources is sent and received as attachments to email. RMC was loaded on each DSS ICP and EOC machines to enable exchange of ADatP-3 and CAP messages operators using DSS. In most cases the

information could be imported into DSS, but the process was not automated and required a significant manual effort by the operator.

The DSS version used during CWID was not the fielded version and was an interim release that had not been fully tested prior to the CWID event. System capabilities were not fully functional. For example, the version of DSS we had could not handle sensor alarms or the new CAP messages so we could not use that part of the system.

Lessons Learned:

Hardware requirements need to be defined early. We believe the startup issue was that the laptops used were on the low end of the acceptable performance range for DSS. The system was apparently still loading even though visually looked like it was completed. We believe we were not waiting long enough for the weddb server to fully come up; we had to wait about 10-15 minutes after the desktop's icons appeared.

DSS can share information outside of its system through file enclosures, but this limits the sharing of information. A series of manual manipulations or retyping of the information was needed to generate CAP and ADatP-3 messages from data entered either in DSS in RMC.

Recommendations:

It would be very helpful if there was some indicator on the server machines to show when they were still loading or actually ready to go. A lot of time was spent trying to connect to the servers when the servers themselves were probably not ready. You would have to open both EOC and ICP systems, and send some test messages/alerts between the two to see if they were syncing.

When using the Hazard Prediction Tool (HPT), the operator needs to enter the GPS coordinates into the tool. The operator may not always be given the GPS coordinates (ie maybe given street intersections) and it would be nice to be able to click on the map and have the lat/long filled in automatically, the operator still needs the option to put them in by hand.

When generating a plume or an ATP-45 using HPT, the operator can only generate one of the models at a time and the tool kicks you out after your selection. When going back into HPT, the settings used to create the last model all go back to default settings, so the operator has to remember which settings were changed when the first model was created. It would be better if HPT didn't kick you out after your model selection and kept the settings the same until you exited out of HPT.

The text alert windows that pop up are small and the window does not expand with the length of the text. We understand that alerts should be short in nature, but it sometimes could be a couple of lines. It would be nice if the text alert pop-up windows were a little bigger to show several lines of text at once instead of scrolling through the alert message.

Recommend transition and incorporation of RMC into DSS to facilitate communications with other civilian and military systems.

5.2.5 Civil Support Team Information Management System

System description*:* The Civil Support Team Information Management System (CIMS) has been specifically designed to meet the needs, requirements, and mission of the nation's Civil Support Teams (CST). The "Digital battle board" capabilities that CIMS provides are:

- share critical incident intelligence and data
- work collaboratively in a doctrine and standards-based environment
- monitor the completion of key team objectives
- accurately record the sequence of incident events

- report to supporting agencies and higher command in a quick and efficient manner

CIMS provides the CST with the ability to direct and monitor the execution of the team's objectives and to present a clear and thorough situation assessment to the on-scene incident commander. Armed with this information, the incident commander is given the best chance of successfully mitigating the situation in a way that can save lives and property, while ensuring the safety of emergency responders and the general public.

As a technology solution designed to support tactical operations, CIMS enables the National Guard CSTs to coordinate the efforts of operations, science, medical, survey, and logistical personnel. CIMS supports the CST mission of assisting civil authorities in understanding and dealing with chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) incidents.

The implementation of the interface with IPAWS OPEN and the ability to generate and process CAP messages was completed just prior to the CWID event. The emphasis was on the functionality related to CAP messaging and not on graphical user interface (GUI) development. The GUI for the fielded CIMS capability is a well thought out and easy to use interface. The CAP GUI implementation provides a fully functional capability, but is more of a developmental interface and needs vetting with the user community.

System performance: The CIMS software was very reliable. The system ran as expected throughout the CWID demonstration. There was a brief time when the mapping module within CIMS was taking a long time to load the pages. Throughout CWID we were using the same incident and all CAP messages that contained coordinates were associated with that incident. When the map took a long time to load, CIMS had 20,000 points in the database. We were able to remedy this occurrence by clearing out the database of those points.

The ability to set the parameters to query for CAP messages was invaluable during testing. This capability was used to query messages over a time range during testing enabling the team to indentify a time related issue associated with Disaster LAN as well as an addressing issue in RMC.

Lessons Learned: Since there is an issue with loading a large number of coordinates on the CIMS map, there needs to be a feature which will enable the user to delete points from the database. Another option would be for the map to load and then allow the user to select the coordinates to load onto the map. This could be done by giving the user the option to load the points during date time group range or load all points.

Another lesson learned when plotting coordinates from a CAP message, the CIMS map would center on the incident coordinates and not on the coordinates loaded from the CAP message. This caused the user to zoom out to find the coordinates that were just loaded. Adjustment should be made to focus the map on the coordinates loaded from the CAP message.

6.0 Hardware Components

6.1 Joint Mobile Command and Training Center

System Description: The JMCTC was a key asset which housed a "Joint Operational Mobil Command Post" environment for on-scene "Command, Control, Computers & Communication (C4). The JMCTC either provides or supports networks to include Wi-Fi & Satellite, VPN and/or non-VPNed web access, and inter/intra system communication. The JMCTC generators provide power to support the JMCTC computer clients, network servers, communications, satellite and display systems, as well as, the equipment (laptops, radios, etc…) the Warfighter (National Guard), civilian government and private sector agencies and personnel bring to the site in support of their mission.

Figure 9 – JMCTC Interior

Figure 10 – JMCTC Exterior

The JMCTC provided the platform for observation, integration, and demonstration for all of the above and unanticipated network and power needs during CWID 11. The platform allowed the exercise participants the ability to visualize the impact of their data in building a common operating picture shared by the DOD, Civil Agency (Federal, State and Local) and Private Sector entities.

The following systems were supported in the JMCTC:

*Software***:**

- **Military** - Systems supported included Command and Control Personal Computer (C2PC); Joint Warning and Reporting Network (JWARN) ; Joint Effects Model (JEM); Decision Support System (DSS) – both EOC & ICP); Civilian Support Team – Information Management System (CIMS); Remote Message Center (RMC)
    - **Messaging Standards:** Allied Data Publication-3 (ADatP-3); United States Text Messaging Format (USMTF)
- **Government** – Integrated Public Alert and Warning System – Open Platform for Emergency Networks (IPAWS/OPEN) ;
    - **Messaging Standards:** Common Alerting Protocol (CAP); Emergency Data Exchange Language – Resource Message (EDXL-RM)
- **Civilian** – Disaster LAN Google Earth; Integrated Chemical, Biological Radiological, Nuclear, Explosive *(ICBRNE)*

Hardware:

- **Communictions:**
    - Handheld devices – iphone, IPad, Android Smartphones
    - Rajant Radios
    - Telegrid Radios
    - BGAN
    - Wi-Fi
    - VPN over Satellite (IP)
    - Voice over Satellite (IP)

- Fax over Satellite (IP)

- **Sensors:**
  - OMNi™ (Compass Systems, Inc)
  - Joint Chemical Agent Detector (JCAD)
  - MultiRae
  - PPb Rae
- **Sensor Networks:**
  - JCID On A Chip (JOAC/Dongle)

The following equipment was supported:

- **Communications:** Satellite, 1.2 Meter Dish, Broadband; VoIP phones (2); Wi-Fi
- **Multi-Screen Video Wall** for Common Operating Picture (4 screens); **LCD TV Displays** (TV Cable News (1); **Streaming Video Screen** for feeds from air assets (fixed wing, helicopter, UAV) and for site security surveillance (9 fixed cameras)

Figure 11 – Multi-Screen Video Wall

- **Video Teleconferencing capability**
- **Power**: External 50AMP 120V; Two 12KW Generators; System Bay UPS
- **Support Power/Network Access for External equipment** and devices requiring external hookups to power and network access (OMNI; Laptops; sensors; Rajants)
- **Mesh Radio Networks** (Telegrid, Rajants, and MU onboard wireless meshnet)
- **Incident Commander Map & Strategy Table**

***System Performance*:** The JMCTC performed exceptionally well. The satellite was called upon as the primary access point to the internet and provided uninterrupted communications.

Lessons Learned: As previously stated the JMCTC performed well and there were no issues of significance related to the vehicle.

6.2 Communications

6.2.1 Android/Smartphones/Tablets

System Description: Systems used during CWID were Android Smartphones and Android Xoom Tablets. These mobile platform technologies were a crucial means of communication between the field operators (National Guard) and the "reach-back" systems being utilized for decision support by analysis's and decision makers. The ability to create alerts and resource requests from the responders on the scene enable the first steps in providing a "trustworthy" flow of information from the scene to the Incident Commanders. Information was shared dynamically to other operational systems being employed to resolve the simulated disasters during exercise.

Alerts and Resource Management messages were created "on-the-fly" by the Warfighters and disseminated via wireless networks to CWID participants. While the MSEL scenarios were designed for the creation and movement of messages between the DOD and other responders (government, civilian first responders and private sector), the strength of the technology for information gathering to capitalize on the strength of the web were not demonstrated. However, operators did experiment with the devices to access information they thought might be useful for "real-time" response.

System Performance: The mobile platform implementation and integration with IPAWS OPEN was a work in progress during CWID. Limited testing was conducted the week prior to CWID and the application was not ready at the start of the demonstration, so RMC was substituted for the first MSEL events. The developers worked throughout the CWID event and were able to complete the implementation of both the CAP and the EDXL-RM on both platforms.

The National Guard Role Players were able to quickly adopt the technologies; all the devices were accepted without resistance or preference to one over another. By the third/fourth time using each device the Warfighters were creating and sending messages without assistance by the technologists who were there for support.

Lessons Learned: The technology was well received by the Warfighters and other emergency management personnel in the exercise. The operators were able to move through the screens to create alerts and resource messages in real-time.

- Technology was well receive and seemed to be easily adopted
- Although the same "fields" exist in the products developing the CAP and RM standard from OASIS, the placement of where those fields appear on the screen vary from product to product. The role players did require some assistance in filling out the form due to time constraints on the MESL play.
- It also appears the "OASIS Standards" for CAP & EDXL-RM need to be tightened to increase the likelihood that products developed independently in the private sector will be able to interoperate. The current standard allows too much flexibility in message creation in regards to required fields/spaces in mandatory fields, etc. The result is disparate productized systems developed in the private sector may not see another vender's (systems) CAP & RM as a valid "well formed" message and not pull the message from IPAWS.
- Actionable information was disseminated quickly
- Apps can be developed for/by emergency management to help streamline the message process
- Technology is relatively cheap as it relates to large emergency management systems and is basically supported by the private sector networks. This alleviates the need for constant and costly maintenance by the user

- The networks are ubiquitous and hence can be used anywhere in the US
- There is still an overarching need for "Technology Introduction" in the Emergency Management arena

***Recommendation*:** Smartphone/Android technology and the creation of "Apps" for emergency management tools should be considered essential for the "technology enabled responder" in the future. iPads/iphones are some of the more popular smartphones being used in the civilian world and as personal communication devices in the military/government world. Future work to investigate and create interfaces should be considered.

The development of Apps should address specific responder roles and tailor the interface to pre-fill or provide a menu driven process to complete message generation to speed the process.

During the time of a disaster, responding organizations should have blanket agreements with manufacturers, suppliers so that "smartphones/tablets" can be purchased and activated as needed. Usually this can be done in very short order. The network backbone will likely be up and running and will have no problem assimilating the devices into the network for immediate use by the responders. With the added usability of a 3G device, users have the existing cellular infrastructure for data as well. The extendibility of mobile handsets combined with the built in features of a camera and email makes them an indispensable asset in the field and promotes "trusted information" exchange to the Incident Commanders at all levels of government.

Mobile platform technology is easy to use and low cost compared to the embedded base of systems used for emergency operations. These devices work as decentralized information platforms that are resilient, easily replaced and improve the decision making capability of management to provide the necessary resources, manpower and technology to the right place at the right time. They increase the level of trusted information by way of providing "firsthand" knowledge for "Situational Awareness and Common Operating Picture" for the analysts and Emergency Operations Center supervisors and command and control personnel charged with resource management and overall situation coordination to affect the outcome.

6.2.2 Rajant Radios

System description: The Rajant radios were used for two uses, one to connect the Joint Chemical Agent Detectors (JCADs) to the network, and the other for connecting to trial 3.07 communications system. The Rajant LX4 radio was physically attached to the passenger's side view mirror on the truck and the Ethernet cable plugged into the truck's network. A Rajant ME2 radio was plugged into the switch on the table with the LCD3s. A second ME2 radio (shown below) was set-up by trial 3.07's truck and plugged into their system with Ethernet cable. BC Commander was being run inside the truck and connected to the same switch as the LX4 radio. BC Commander is the Rajant software that monitors the wireless network and used to change radio settings and parameters.

Figure 12 – Rajant Radio

System performance:

The system performed very well. The radio by trial 3.07 was around the corner of the building and had no line of sight; we thought we would need another radio to go around the corner. No additional radio was needed to make that connection.

When alarming the LCD3s, the alarms showed up in JWARN, and the BC Commander software was showing a solid connection to the radios at the times we were checking it.

Lessons Learned:

Although we knew this already, when changing settings/parameters on the radios, do the one connected to the bc commander last. If you do that one first, you may have trouble connecting to the other radios since the settings are different (ie, ip addresses, channels).

Recommendations:

The NBCBMB has a great deal of experience working with Rajant radios and there were no major issues experienced during the CWID event.

6.2.3 Telegrid Radios

***Description*:** The Telegrid WZRDnet hand-held mesh network is a unique system for deployment to military personnel or any other group seeking a rapidly deployable, portable communications solution. Comprised of small hand-held access points and a gateway, this system can provide push-to-talk radio infrastructure, GPS location finding, text messaging, and data transmission over several square kilometers while having superior battery life and requiring no external communications link.

Figure 13 – Telegrid Radio

The system was set up and deployed for use and demonstrated with the JMCTC truck at CWID 2011. For this scenario, the WGW-330 Gateway, six WHD-310 Handsets, and a PC running the WZRDchat program were used.

System performance:

- Two warfighters were shown how to use the handsets for push-to-talk audio communications, text messaging, and GPS location/tracking. They used the radios throughout the parking lot

complex for approximately ½ hour. The GPS application was accurate to within a few meters on the display. Push-to-talk audio worked very well.

- A net-book PC running the WZRDchat program was set up and connected to one of the handsets. Several other handsets were on display for demonstration to the various defense groups that came through during the day.
- Monmouth University and CERMUSA worked on configuring the Gateway for use with the Public Switched Telephone Network (PSTN) lines available on the JMCTC truck. Due to the Gateway being connected through a Cisco call manager/router and the satellite link back to MU, we ran into some issues making the telephone patch work correctly. Specifically, we were not able to cause the proper delay after a number was dialed to automatically enter the PIN as a Suffix. This PIN code is required by MU for dialing long distance numbers from their PBX. Calls to four digit extensions on campus and 1-800 numbers worked fine from the TELEGRID handsets. Telegrid was contacted to inquire about adding additional delay to the Suffix. Each "w" added before the number will add ½ second delay. The problem is believed to be a combination of the Cisco call manager and the latency of 600mS through the satellite link.

Lessons Learned:

Two improvements/changes to the handsets were noticed throughout the CWID exercise. First, the small display needs to be much brighter for viewing in direct sunlight applications. A transflective display was recommended by one of the vendors present because it reflects more natural sunlight and consumes less battery power due to a lower wattage backlight being needed. Second, the ability to dial additional digits after a telephone call is placed from the handsets is not there. For example, this would be used to dial a PIN or interact with voice prompts with a computer on the far end. No such ability exists with the handsets now. Once a call is established, only the PTT button is active for the duration of the call.

6.4 Sensors

6.4.1 Joint Chemical Agent Detector. The Joint Chemical Agent Detector (JCAD) is a standard military, hand-held device intended to automatically warn users of the presence of chemical agents. The JCAD uses Ion Mobility Spectrometry technology to detect, identify and quantify these chemical agents.

Figure 14 – Joint Chemical Agent Detector

There were two JCAD set-ups used. The first was for JWARN. Each JCAD's data cable was connected to a Universal Serial Bus (USB) to Ethernet device server (small box with 4 USB and 1 Ethernet slots) which was connected either to the network, or through the Rajant radios (both ways were done successfully). This device server USBs were controlled/activated by software on the JoaC laptop and was the way the dongle software received the JCADs message flow. The JoaC software then converted JCAD's messages into JWARN to JMAS (JWARN Mission Application Software) Interface (JJI) format so that the messages could be sent and read into JWARN. JWARN would then display JCAD's status (alarming, cleared, disconnected, etc) properly on the map or under the JCID tree area. Two JCADs were used in this set-up.

The other JCAD was hooked up with the OMNi^{TM} system using the data cable. When the JCAD went into alarm, it would send the information to the OMNi^{TM} system where it was addressed to forward the information to either JWARN or DisasterLAN (depending on the scenario being played).

System performance: The system performed very well. The JCAD's alarms were shown in JWARN under the JCID's area under JWARN, and on C2PC's map, along with the audible alarm. The JCAD being used with OMNi^{TM} system also went smoothly and the JCAD alarms were received by OMNi^{TM}'s server where other systems could retrieve it.

Lessons Learned: The NBCBMB has a great deal of experience working with the JCAD and there were no issues experienced during the CWID event.

Recommendations: The NBCBMB has a great deal of experience working with JCADs and there were no major issues experienced during the CWID event.

6.4.2 MultiRae.

System description: The MultiRAE Plus is a chemical, vapor, point detector that combines a photoionization detector (PID), Lower Explosive Limit (LEL), O_2 and two other variable gas sensors into one device. The MultiRAE has an internal sampling pump to draw the air in for continuous air monitoring. The MultiRAE was one of the sensors used with ICBRNE to send a chemical alarms through the system. This was done by attaching an ICBRNE dongle to the detector and plugging in the data cable into the dongle. Then a simulant was used to have the MultiRAE go into a chemical alarm.

Figure 15 - MultiRae

System performance: The O_2 Sensor was constantly in alarm. It was believed that the sensor module was bad and needed to be replaced, or it needs to be recalibrated. ICBRNE did show the alarm in their system.

6.4.3 PPb Rae.

System description: The PPbRAE Plus is a photo-ionization detector (PID) to detect chemicals. The PPbRAE has an internal sampling pump to draw the air in for continuous air monitoring. The PPbRAE was the main sensor used with ICBRNE to send chemical alarms through the system. This was done by attaching an ICBRNE dongle to the detector and plugging in the data cable into the dongle. Then a simulant was used to have the PPbRAE go into a chemical alarm.

System performance: The PPbRAE alarmed when the simulant was used (a dry board marker), but as CWID progressed, it took a little longer to alarm the detector since the dry marker was not as potent as it was in the beginning. The alarms showed up in ICBRNE as expected.

The ICBRNE personnel had a great deal of experience working with the PPbRAE detector and there were no major issues experienced during the CWID event.

Figure 16 - PPb Rae

6.4.4 Operational Mapping and Networked Intelligence (OMNi™)

Description: The OMNi™ is a hand-held device for mobile mapping and expedited reporting. This is a geo-spatially aware device employing a GPS antenna, a Laser Range Finder, and a wide array of interchangeable sensors including day/night cameras. In that regard, the unit is not a specific product, but a widely ranging capability for numerous requirements.

Figure 17 - OMNI™

The OMNi™ enables the user to collect precise geo-tagged intelligence from a standoff position. This allows tagging the coordinates with voice, audio/video, environmental data and text information into an embedded GIS. It can be used to capture data on land, sea or air. A key feature is that the information is posted immediately to the internet using Google Earth™. This real-time exchange of enriched data enables multiple agencies to coordinate and streamline response efforts efficiently while tracking and monitoring events geo-spatially.

Prior to CWID, the OMNi™ was used to survey the damage in American Samoa following the tsunami, Hurricane Katrina in New Orleans and even the BP oil spill in the Gulf of Mexico. In the case of the oil spill, a team was deployed to Florida to survey the shoreline for any oil evidence. After discovering tar balls in the sand, the OMNi™ then collected GIS, audio and video data which was then communicated to the hazmat teams for proper clean-up and disposal.

The Integration of the JoaC and RMC was completed prior to CWID enabling the sharing of chemical detection data and CAP messages. For CWID Trial 2.32, the OMNi™ was used to provide field data that included audio captures, video, still imagery, areas of interest in the form of mapped polygons. The integration of RMC enabled OMNi™ to share CAP messages with polygon information with RMC operating in the JMCTC via email. The integration of the JoaC software provided the capability to take in JCAD raw data, parse the alarm data into a JII format, and pass the JJI to JWARN. Compass successfully completed these integration efforts in less than one month.

Even though the OMNi™ only participated at the Herndon CWID location, the MSEL locations were across the U.S. To participate in multiple locations, Compass Systems pre-loaded offsets for all of the MSEL's into a table for the user to select from. Once selected, the user would then be virtually placed into one of the remote MSEL locations in which to collect data.

System Performance: The personnel assigned to use the OMNi™ were very pleased with the performance of the device. Many of the users and CWID administrators referred the OMNi™ as the wow factor in its simplicity and meaningful results in utilizing the JCAD interface.

For the JCAD, the process was completely automated. Once the JCAD was triggered, the OMNi™ gave a series of alarms and easy to follow directions to send the alert to the JWARN server.

The period to train the CWID users was less than 30 minutes on average. By the second MSEL, the user was comfortable in the use of the device. This was largely a direct result of the menu driven or automated approach to collecting data.

Each MSEL represented different scenarios to include: taking a video, adding an audio clip, using a polygon to capture multiple points and use of the JCAD reader. Compass Systems would simply instruct the user to collect different media for each MSEL. This allowed for a myriad of data placed onto a Google Earth™ map and also allowed the operator to share CAP messages with the ICP and EOC.

Recommendations: The main recommendation given to Compass Systems was that the OMNi™ needed to be more compact and lightweight. In its current state, the OMNi™ weighs over 6 pounds and utilizes an external battery. During the exercise, a tripod was utilized to steady the device due to the size and weight. There was also mention about the glare on the LCD display in sunny conditions.

Compass Systems is in the process of completely redesigning the OMNi™. The effort will yield a unit that weights approximately 2 pounds and will be one third of the current size. This will allow for a completely hand held device

without the use of a tripod. Compass Systems Inc. will also be including the latest technologies for GPS, cameras, batteries and anti-glare displays.

The new OMNi™ is presently in the design phase. The build phase should begin the last quarter of 2011. We are anticipating a product launch first quarter 2012.

6.5 Sensor Network Interface

6.5.1 JCID-on-a-Chip (JoaC)

Description: Dongles are JoaC devices or SW developed by ECBC to take the data flow from sensors and put the data in the JWARN JCID Interface (JJI) format so JWARN can display the results. For this exercise, we used the software version of the JoaC. There were 5 versions of the JoaC software used on the JoaC laptop which had the different positions of the JCADs (GPS coordinates were virtualized to show their exercise locations and not actual location in Herndon VA). Three were in Charleston SC, and two in Aberdeen Proving Grounds; both locations were for the hurricane scenario. The detector used for this exercise was the JCAD which is a chemical point vapor detector using Ion Mobility Spectrometry techniques for identification of chemical hazards.

The LCD3s were connected to a USB to Ethernet device server (small box with 4 USB and 1 Ethernet slots) which was connected directly to the network, or through the Rajant radios (both ways were done successfully). This device server had software on the JoaC laptop to control/activate the USBs for use by the JoaC laptop and was the way the JoaC software received the LCD3s message flow. This device was used so the JoaC laptop did not have to be co-located with the sensors and to have a way to connect the LCD3s to the network. The JoaC and JWARN laptops were also connected to the network from within the truck.

System performance: With the exception of Norton antivirus shutting down the device server, the set-up performed well. Five copies of the JoaC software were used because we had several sensors at five different locations which had to be hard coded to virtualize the GPS positions of those sensors, but only a maximum of 3 were running at one time (that was the number of sensors used in Charleston SC). The sensor positions showed up in JWARN in the right locations, and the alarms were displayed correctly in JWARN.

Lessons Learned: Before running the JoaC software, the USB to Ethernet device server's software had to be running on the JoaC laptop and have the USBs that were being used for the scenario activated before running the JoaC software. You also needed to have the LCD3s running before running the JoaC software; otherwise it would not "see" the detector. Sometimes the USB to Ethernet device server would deactivate the USB ports being used after 10-20 minutes of running. It turned out that Norton Anti-virus was deactivating these ports for some reason.

Recommendations:

Modify the JoaC software so it doesn't matter if the JoaC software is running before the sensor comes on-line. There are times when the LCD3 may have to be rebooted which would also mean the JoaC software would also have to be restarted, and would be a little tricky if the two are not co-located. You could also have power interruptions which would cause a problem.

If using the USB to Ethernet device server, you'll need to turn off Norton antivirus software.

7.0 CWID Scenario Development

Scenarios were created to show how our systems could be used in an emergency situation. Several of the scenarios were designed by the CWID staff (Days 2, 4, 5 and 9) while the rest were off-shoots of some of the other CWID

scenarios and were developed by our team. Several of the scenarios were also repeated for the second week (Days 1 & 6, and Days 3 & 8) to keep the work load down and to build some familiarity with the operators. To aid the scenario writing process, the team developed time lines and flow diagrams to map the message/information flow based on the system to be used and the role player to perform an action.

Each scenario would have a list of role players who play a part of the recovery effort. The people who played the role players in Herndon VA were the National Guard, and most of the time each National Guard person had 3-4 role player positions they were playing. By the middle of the exercise, our team was allowed to be role players to help ease the burden for the National Guard personnel. Each role player had the steps and information needed to use the system they were on to input and share information between military and civilian systems.

The following is a list of scenarios with a short description that ran each day:

Day 1 – Fire in Cleveland National Forest, CA

911 receive multi phone calls of fire and smoke in area of Japatul Valley Road, Japatul Road and route 8 in Cleveland National Forest. San Diego County Fire Department deploys for initial response.

Day 2 – Biological Attack at Reagan National Airport's Metro Station

There is an explosion at the Reagan National Airport Metro Station. County Emergency Manager activates EOC. First responders call in to County EOC to report on situation. County EOC receives information and is shared with surrounding communities. First responders set up an on-scene CP at Aviation Circle and want a ½ mile radius cordon put into place. Initial determination of damage is no major structural damage, many injuries and deaths. Initial witness reports indicate several bombs going off blowing out the side of several rail cars.

Day 3 – Chemical Attack at US Navy NRSW base in San Diego, CA

Fuel truck (loaded with GB) drives down East Harbor Drive and detonates the truck at South 32nd Street and East Harbor Drive in San Diego CA. Explosion causes severe damage to personnel and surrounding structures on US Navy NRSW base.

Day 4 – Hurricane Anna

Part 1 - In preparation for Tropical Storm Anna, an inspection of Aerial Port Squadron Bldg on base (lat 32 deg, 53' 25.54", long -80 degrees, 3' 4.51") and uncovered a building that is damaged with no power or environmental controls. During preparation in anticipation of Tropical Storm Anna at the Aerial Port Squadron building, a forklift operator punctures a ton container, later to be found filled with chlorine. Operator smells something but can't identify it and informs the EOC

Part 2 - During preparation for Tropical Storm Anna, the Chemical Demilitarization Facility at Aberdeen Proving Ground (APG), MD sustained damage to the filtration system for the Ton Container Drain Facility. Several ton containers filled with nerve agent were being drained at the time the filter unit was damaged. No status as to extent of the damage at the time, but Tech Escort has been called to the site to evaluate the situation.

Day 5 – Explosion at Petco Park San Diego, CA

A massive explosion occurs on a street adjacent to Petco Park San Diego, CA during a nationally televised baseball game, caused by a truck carrying a fertilizer bomb with mustard chemical agent. There is massive destruction to the ballpark and surrounding buildings as well as mass civilian casualties. The San Diego Co, CA EOC Operations Officer provides notification to the other affected jurisdictions.

Day 6 - Fire in Cleveland National Forest, CA

911 receive multi phone calls of fire and smoke in area of Japatul Valley Road, Japatul Road and route 8 in Cleveland National Forest. San Diego County Fire Department deploys for initial response.

Day 7 – Radioactive Steam Release at Calvert Cliffs Nuclear Plant, MD

Pumps at the Calvert Cliffs nuclear power plant get turned off with all indicators showing they are still on-line. Relief valve emits radioactive steam into the atmosphere. External sensors go into alarm in control room that a release was made outside of the building. Assume RMC being used at plant and wind blowing west to east.

Day 8 – Chemical Attack at US Navy NRSW base in San Diego, CA

Fuel truck (loaded with GB) drives down East Harbor Drive and detonates the truck at South 32nd Street and East Harbor Drive in San Diego CA. Explosion causes severe damage to personnel and surrounding structures on US Navy NRSW base.

Day 9 – Hurricane Anna

Part 1 - The Charleston AFB EOC Ops Officer reports in the aftermath of Tropical Storm Anna that during an inspection of Aerial Port Squadron Bldg on base (lat 32 deg, 53' 25.54", long -80 degrees, 3' 4.51") and uncovered a building that is damaged with no power or environmental controls. During clean-up of Aerial Port Squadron building a forklift operator punctures a ton container, later to be found filled with chlorine. Operator smells something but can't identify it and informs the EOC

Part 2 - The aftermath of Hurricane Anna is being felt up and down the east coast. The Chemical Demilitarization Facility at Aberdeen Proving Ground (APG), MD sustained damage to the filtration system for the Ton Container Drain Facility. Several ton containers filled with nerve agent were being drained at the time the filter unit was damaged. No status as to extent of the damage at the time, but Tech Escort has been called to the site to evaluate the situation.

8.0 Pre-Execution Planning

The vast majority of the effort involved in a successful CWID is expended before the event takes place. Three required planning conferences were attended in Williamsburg, VA. The planning conferences were used to monitor the individual trials progress and readiness for CWID execution. Additionally, the planning conferences were used to identify interoperability opportunities with other trials and identify site specific requirements for each trial. Since DHS S&T was the sponsor for Trial 2.32, the decision was made to deploy to the DHS Battle Lab as the primary trial site. Two site visits were made to the Battle Lab to coordinate space, power, and network connectivity.

All systems were set up at ECBC prior to deployment for CWID. The purpose was to complete integration, verify communication pathways, support training material development, support MSEL development and to dry run MSELs. Beginning in the February/March time frame software and hardware tools began to arrive at ECBC and familiarization with the individual tool sets began. A stand alone network was setup with internet access provided by the ECBC UUNET connection. A mail server was set up to allow message sharing between JWARN and the Remote Message Center. Individual demonstrations were provided by subject matter experts for each of the technologies as needed. Specifically, Compass, SPAWAR, PM Guardian, Opti-Metrics, Ensco, EMCS, and Monmouth University all visited ECBC to provide training, integration support, and MSEL development support.

The JMCTC truck arrived at ECBC in mid-May so network connections could be worked, work station layout developed, system integration, and MSEL dry runs could be completed. The truck was moved to the DHS Battle Lab on 31 May 2011. System set up took place 31 May to 3 Jun 2011 and CWID execution began on 6 Jun 2011. Role player training was conducted 2 to 3 hours each day during the setup period. Virtual training of role players at Hanscom and NORTHCOM was conducted via teleconference for approximately one hour.

CWID Training - The CWID Training activities included development of training materials for each technology, on-site training with the DEARNG, on-site training at Herndon, and virtual training with the virtual sites.

9.0 CWID Execution

CWID execution took place 6 – 16 Jun 2011. CWID was a successful demonstration for Trial 2.32 M2CM. During the course of CWID, Trial 2.32 – M2CM was able to demonstrate exchange of messages between civilian and military responders. The end to end exchange of information from the sensor level to the EOC was also successfully demonstrated. Role players from the DEARNG and NJ National Guard received training in the operation of each of the technologies and were able to successfully operate each by the end of the CWID scenario play. The trial was a particularly complex undertaking in that there were multiple systems that each individual role player needed to be trained on. This made the performance by the role players all the more impressive, since they were able to move between technologies each day and perform in some cases very different functions.

There were multiple plans in place to gain network access to include the DHS Battle Lab's access point , Trial 3.07, BGAN, and JMCTC truck satellite. Ultimately, the JMCTC satellite was used for the majority of the trial.

CWID-U Network - Our main plan to connect into CWID-U's unclassified network and the internet was to go through the wireless access point on the top of the DHS Battle Lab's building. To keep our IP addresses from changing, we used a router with a built in DNS server as a gateway to forward our requests. From there, Virtual Private Networks (VPNs) were used to connect to the other sites on the CWID-U network. The connection to the internet was needed for access to IPAWS/OPEN server, Disaster LAN website, Google earth, ICBRNE's server, and OMNI's servers. The connection to CWID-U was needed to connect to the other role players that were using RMC and JWARN, and for CWID's mail server. The access point was not available for use until Monday of the second week due to getting the hardware in and then setting it up. Setting up the access point was not a high priority for Herndon at the time.

On Monday and Tuesday of the second week, we tried using the access point and had issues with it. Some systems were able to connect to others some of the time, and others had trouble all the time connecting. The connection speeds sometimes ran slow when the systems were connected to the internet. No pattern was found that would help explain this behavior. We also had instances of emails not being received at the remote sites. By the end of the day on Tuesday, it was decided to use the truck's satellite system for the rest of the trial which increased the reliability of the connections, but was slower. We figured the VPN's bandwidth was very narrow for the amount of traffic trying to get through and would be better off doing something else. Gmail accounts were created and used for our systems (except for San Diego site, they could get our emails on their email server). In San Diego, the role players had two email accounts, one for their outlook and one for RMC/JWARN system. The problem they had with one account was either RMC/JWARN system would take the message from their outlook account before they could read them, or if they read them in outlook, it would not be readable in RMC once it was transferred to RMC. The decision was made to have two email accounts for these role players, one for Outlook and one for RMC messages. Everything worked, but it was slower than the CWID-U network. Disaster LAN had speed issues on the truck's satellite and ended up using a private wireless card to get access to the internet. ICBRNE and OMNI did not have issues because they did not use the CWID-U network to send their sensor information to their servers.

Interoperability - Trial 3.07 (Tactical Coalition Gateway – TCG)

Our back-up plan to connect into CWID-U's unclassified network and the internet was to use trial 3.07, Tactical Coalition Gateway (TCG). We would use the Rajant radios to send the traffic to their van located around the side of DHS Battle Lab's building in Herndon VA and hook into their system by Ethernet cable. Our traffic would then go through the satellite to hit TCG's set-up at U.S. NORTHCOM's site in Peterson's AFB CO to get into the CWID-U network and the other CWID participates. This would be our access into the CWID-U network if the access point on the building did not come through.

TCG did not show up at the Herndon site until the first Thursday (June 2) and they were busy between setting up their equipment at Herndon as well a second site they were working on. Friday was the training day for the operators for both TCG and our trial, so no CWID-U connection attempts were made by our trial during the first week.

During the second week, TCG had some satellite tracking issues with their hardware, but by Wednesday morning (June 8) we were ready for a test. We were able to ping TCG's gateway machine in Peterson's AFB, but we could not get into CWID-U or the internet. Upon inquiring on the status at Peterson's AFB, TCG had hardware issues there as well as having their requested frequencies denied and given new ones to work with. New frequencies required new equipment which they had to get into place. At the end of the second week, we got closer, but still could not get on CWID-U or the internet due to their all their issues.

In the final week, TCG was still having hardware issues, plus once the new hardware was in place, they had a few alignment issues to deal with. With these and the tours that came through on both ends, TCG was not ready for another test until the last day of the exercise. Near the end of the day we tried one more test to hit CWID-U and the internet, but were not able to hit TCG's gateway in Herndon VA. We feel we were close in getting the connection, but we ran out of time trying to share messages with other sites using TCG's access to CWUD-U and the internet.

MSEL Play – Execution of the MSELs play progressively improved as the operator became more familiar with the systems and set up and connectivity issues were addressed. Since the MSEL play involved role players from multiple sites, coordination between sites was necessary to verify messages were being received. During the first two or three days there were issues with network connectivity in both Herndon and in San Diego. Using the CWID email address became an issue with the Remote Message Center in San Diego. The role player would open the message in Outlook interrupting the Remote Message Center polling so the messages wouldn't make it to the message center. At the other sites the port assignments were not identified so it became expedient to set up Gmail accounts for each role and use those for the email exchange of messages between JWARN and the Remote Message Center.

Once the connectivity and email issues were worked MSEL play was greatly improved, but it quickly became obvious the timing of events was not adequate to allow the role players to move between systems and complete the tasks required. The decision was made to have a few of the Trail partners supplement the two role players in the JMCTC and allow them to concentrate on mastering one or two technologies each day. The role players still worked with all technologies over the course of the demonstration, but within any one day they were limited to one or two tools that had the most significant play on any one day. The time interval between events was still too short to maintain the timeline, but all tasks were being completed.

10.0 Conclusions and Recommendations

Trial 2.32 – M2CM was successful in meeting the primary objective to demonstrate the exchange of information across a combination of existing military, civilian, and emerging S&T Tools. Role players from the DEARNG and New Jersey National Guard after being trained on the various technologies and successfully generated, sent, and received CAP, EDXL-RM, and ADatP-3 messages using the Civilian and Military tools.

The M2CM CWID Trial was a standards based system of systems approach to bridge the information gap between disparate systems in different operational domains (Civilian and Military). Using the Remote Message Center as the transition point between the Civilian standards (CAP and EDXL-RM) and military messaging (ADatP-3) in conjunction with the IPAWS OPEN, the ability to share information between multiple information management systems in both domains was demonstrated during CWID 2011.

Operationally the M2CM demonstrated the ability to rapidly share information across the military and civilian domains. Exchange of information has been limited by incompatible messaging and information management systems, but the M2CM trial demonstrated the initial bridging of the information gap by providing a transition

capability in the form of the Remote Message Center. The transition capability allows the Military and Civilian emergency management communities to quickly distribute alerts, warnings, and resource information to local, state, and federal agencies using various applications compatible with Military or Civilian standards. M2CM was among the first to push data through IPAWS OPEN. It went operational the week before CWID.

The JMCTC provided a flexible platform for the collaborative effort between the Mil/Gov/Civil role players. The adaptability of the JMCTC to be configured for different operational environments was demonstrated as different network connections were used during the pre-CWID testing and CWID Execution. The JMCTC was a valuable asset during CWID that needs to stay current with leading edge technology.

Trial 2.32 – M2CM was truly a collaborative team effort that brought representatives from multiple Military, Federal Government, and commercial organization to address a common goal of information sharing. The first and most critical recommendation is to continue this multi-sector collaboration. Recommendations for specific tools were provided in the individual write ups.

Appendix 1

Contact Information

Trial 2.32 Managing Military Civilian Messaging (M2CM)
Contact List

Organization	System/Role	Point of Contact
Department of Homeland Security – CB S&T Branch	Trial Sponsor	Christopher Russell Christopher.E.Russell@HQ.DHS.GOV (703)647-6020
Edgewood Chemical Biological Center	Trial Lead	William Ginley William.ginley@us.army.mil (410)436-5649
	Trial Execution	Donald Macfarlane Donald.macfarlane@us.army.mil (410)436-5876
	Trial Execution	David Drummond David.drummond1@us.army.mil (410)436-5602
Buffalo Computer Graphics	Disaster LAN	Christopher Zak – POC 3741 Lake Shore Road Blasdell, NY 14219 (716) 822-8668
Compass Systems, Inc.	OMNi	Tad Britt Program Manager Compass Systems, Inc. 2001 S First St. Suite 107-B Champaign, IL 61820 Tel / Cell (217) 552-2478
FEMA/NCP IPAWS (Contractor)	IPAWS OPEN	Gary Ham Eyestreet Solutions, contractor FEMA/NCP IPAWS Systems Architect, IPAWS-OPEN Mobile Phone: 703-899-6241 e-mail: gary.ham@eyestreet.com
FEMA (Contractor)	Trial Execution	Tom Ferrentino tferrentino@verizon.net (716) 656-0540

Organization	System/Role	Point of Contact
Installation Protection Program	Decision Support System	Brent Butowsky Brent.butowsky@us.army.mil (703)962-0669
IUP Research Institute Business and Technology Group Inc.	CST Information Management System (CIMS)	Patrick Higgins 280 Indian Springs Rd Suite 116 Indiana, PA 15701 higgins@iupri.com 724.463.8315 x112
		Brian Petersen 280 Indian Springs Rd Suite 116 Indiana, PA 15701 petersen@iupri.com 724.463.8315 x111
OptiMetrics, Inc.	Remote Message Center	Jack Berndt Director, CBRN Software Development OptiMetrics Inc (410) 569-6081 ext 119 jberndt@omi.com
Rapid Response Institute Monmouth University	Command Truck Handhelds	Dr. Barbara Reagor Director, Rapid Response Institute Monmouth University breagor@monmouth.edu 732.571.3511 (H) 732.610.1001 (C)
		Jim Hammill Senior Researcher, Rapid Response Institute Monmouth University jhammill@monmouth.edu 302.644.9539 (H) 908.343.4343 (C)
SPAWAR Systems Center Pacific	ICBRNE	Bruce Plutchak - Government SPAWAR Systems Center Pacific bruce.plutchak@navy.mil (619)553-3658

Organization	System/Role	Point of Contact
SPAWAR Systems Center Pacific	ICBRNE	Ritesh Patel - Government SPAWAR Systems Center Pacific ritesh.patel@navy.mil (619)553-4509
		Doug Hardy - Government SPAWAR Systems Center Pacific douglas.hardy@navy.mil (619)553-5410
		Francis Cortez - Government SPAWAR Systems Center Pacific francis.cortez@navy.mil (619)553-3663